Representasjoner av den Modulære Gruppa

av

Håkon Hobæk

KORT MASTEROPPGAVE

for graden

Master i Matematikk

(Master of Science)

Det matematisk- naturvitenskapelige fakultet

Universitetet i Oslo

Mai 2009

Faculty of Mathematics and Natural Sciences

University of Oslo

Innhold

1 Introduksjon

Representasjonsteori er et område innenfor matematikken hvor man representerer elementer i grupper og algebraer med lineære transformasjoner av vektorrom. I lineær algebra finnes det mye verktøy, og dette kan man bruke til for eksempel å finne undergrupper. Ved å benytte matriser kan man forenkle regningen eller ta i bruk dataprogrammer som regner ved hjelp av matriser. For noen typer grupper, for eksempel endelige og kompakte, er det en fyldig teori som fyller mange bøker. For andre typer grupper, for eksempel uendelig diskrete grupper, finnes det ikke en stor generell teori. Denne oppgava legger hovedvekt på endeligdimensjonale representasjoner av den modulære gruppa og noen av dens undergrupper.

Etter en introduksjon til den modulære gruppa og representasjonsteori, kommer et kapittel om traseringen. Det vises, ved hjelp av Cayley-Hamiltons teorem, at man kan skrive trasen til potenser av matriser som lineære kombinasjoner av matriser av lavere potens. Dette fører til at karakteren til representasjoner av en uendelig gruppe kan bestemmes ut ifra karakteren til et endelig antall elementer. De mest interessante representasjonene er de irredusible, og alle klassene av 1-, 2- og 3-dimensjonale, irredusible representasjoner blir funnet i kapittel 5. Det blir også gitt konkrete eksempler på irredusible representasjoner av undergrupper som for eksempel S_3. Til slutt er det et kapittel om ekstensjoner og hvordan dette kan brukes til å finne indekomposable representasjoner. Ved hjelp av to representasjoner av dimensjon n og m kan man konstruere en indekomposabel representasjon av grad $m+n$.

Den modulære gruppa er en uendelig, diskrete gruppe generert av to variable. For generatorene a og b i den modulære gruppa er $a^2 = 1$ og $b^3 = 1$. På grunn av dette vil vi i utregningene ofte støte på enhetsrøtter av grad 2, 3 og 6. Vi vil derfor bruke notasjonen $1 \neq \omega = \sqrt[3]{1}$, en rot av $x^2 + x + 1$, og $-1 \neq \nu = \sqrt[3]{-1}$, en rot av $x^2 - x + 1$, gjennom hele oppgava.

2 Grupper

En **gruppe** G er en mengde lukket under en binær operasjon
$* : G \times G \longrightarrow G$ slik at:

(i) $(s_1 * s_2) * s_3 = s_1 * (s_2 * s_3)$, $\forall\ s_1, s_2, s_3 \in G$

(ii) Det eksisterer et element $e \in G$ slik at $e * s = s * e = s$, $\forall\ s \in G$

(iii) For hver $s \in G$ så eksisterer det en $s^{-1} \in G$ slik at $s^{-1} * s = s * s^{-1} = e$

Enkle eksempler på grupper er $\mathbb{Z}$ med addisjon, $GL_2(\mathbb{C})$ med multiplikasjon og $\{1, \omega, \omega^2\}$ med multiplikasjon. $|G|$ kalles **ordenen** til gruppa og er antall elementer i gruppa. Begge de første eksemplene er grupper av uendelig orden, mens det siste eksemplet har et endelig antall elementer og er en gruppe av orden 3. Vi sier at ω er en **generator** for den siste gruppa ettersom alle elementene i gruppa er potenser av ω, mao: de er generert av ω. Lar vi $s \in G$ og det eksisterer en $n \in \mathbb{N}$ slik at $s^n = e$ og $s^m \neq e$, $\forall\ m \in \mathbb{N}$, $m < n$ sier vi at s har grad n.

En **monoide** er en mengde med assosiativ multiplikasjon og en enhet. Med andre ord en mengde M hvor (i) og (ii), men ikke (iii), er oppfylt. Gitt en mengde A, så er den **frie monoiden**, også kalt **mengden av ord** på A, mengden $W(A)$ av endelige sekvenser av elementer fra A. I $W(A)$ er produktet gitt ved skjøting av ord og enheten er det tomme ordet. Et element $w \in W(A)$ ser typisk ut som $w = a_1 a_2 .. a_n$, hvor $a_i \in A$. Lengden av ordet er n og det tomme ordet er det eneste ordet med lengde 0. Vi identifiserer A med mengden av ord med lengde 1.

La $(G_i)_{i \in I}$ være en familie av grupper. La A være den disjunkte unionen $A = \coprod_{i \in I} G_i$. La $\sim$ være ekvivalensrelasjonen på $W(A)$ definert ved

$we_iw' \sim ww'$ når e_i er enheten i G_i for en $i \in I$

$wabw' \sim wcw'$ når $a, b, c \in G_i$ med $ab = c$ for en $i \in I$

for alle $w, w' \in W(A)$. Kvotienten $W(A)/\sim$ er en gruppe og blir kalt det **frie produktet** av gruppene G_i $(i \in I)$ og skrives $*_{i \in I} G_i$. Den inverse til et element $a_1 a_2 ... a_n$ i $*_{i \in I} G_i$ er $a_n^{-1} a_{n-1}^{-1} ... a_1^{-1}$. Et ord $w = a_1 a_2 ... a_n \in W(A)$ med $a_j \in G_{i_j}$ sies å være **redusert** hvis $i_{j+1} \neq i_j$ $(1 \leq j \leq n-1)$ og a_j ikke er et enhetselement. Lar vi for eksempel $I = \{1, 2\}$, $G_1 = \{e_1, a\}$ og $G_2 = \{e_2, b, b^2\}$ så er $abab^2aba$ på redusert form, mens abb^2a og ae_2 ikke er det.

Lemma 1 (Ping-pong-lemma). *La Γ være en gruppe som virker på en mengde X, G_1, G_2 være to undergrupper av Γ av henholdsvis orden minst 3 og 2, og la G være den undergruppa generert av G_1 og G_2. Anta at det eksisterer to ikke-tomme undermengder X_1 og X_2 i X med $X_2 \not\subseteq X_1$, slik at*

$$\begin{aligned} gX_2 &\subset X_1 \qquad \forall g \in G_1, \quad g \neq 1, \\ gX_1 &\subset X_2 \qquad \forall g \in G_2, \quad g \neq 1. \end{aligned}$$

Da er G isomorf med det frie produktet $G_1 * G_2$.

Bevis. La w være et ikke-tomt redusert ord med bokstaver fra den disjunkte unionen av $G_1\backslash\{1\}$ og $G_2\backslash\{1\}$. Vi må vise at elementet i G definert ved ordet w ikke er 1.

Hvis $w = a_1b_1a_2b_2...a_k$ hvor $a_i \in G_1\backslash\{1\}$ og $b_j \in G_2\backslash\{1\}$ for alle i og j så er

$$\begin{aligned} w(X_2) &= a_1b_1a_2b_2...a_k(X_2) \subseteq a_1b_1a_2b_2...a_{k-1}b_{k-1}(X_1) \\ &\subseteq a_1b_1a_2b_2...a_{k-1}(X_2) \subseteq ... \subseteq a_1(X_2) \subseteq X_1 \end{aligned}$$

og ettersom $X_2 \nsubseteq X_1$ så kan ikke $w = 1$.

Hvis $w = b_1a_1b_2a_2...b_k$ velg en $a \in G_1\backslash\{1\}$. Da er $awa^{-1} \neq 1$ ved forrige argument og $w \neq 1$. Hvis $w = a_1b_1a_2b_2...a_kb_k$, velg en $a \in G_1\backslash\{1, a_1^{-1}\}$ og argumenter med awa^{-1} igjen. Hvis $w = b_1a_1b_2a_2...a_k$, velg en $a \in G_1\backslash\{1, a_k\}$ og gjør det samme. □

Det finnes mange grupper generert av to elementer av orden 2 og 3. Den minste er S_3 og den største er det frie produktet $\mathbb{Z}_2 * \mathbb{Z}_3$. I mellom fins det mange grupper og en samlebetegnelse for noen av dem er (2,3,p). Det er gruppa som er generert av to elementer a og b hvor $a^2 = b^3 = (ab)^p = 1$. For $p = 2$ er $(ab)^2 = 1$. Det vil si at $aba = b^{-1}$ og gruppa $S_3 \sim (2, 3, 2)$.

2.1 Den modulære gruppa

En funksjon $f : \mathbb{C} \longrightarrow \mathbb{C}$ gitt ved

$$f(z) = \frac{az+b}{cz+d}, \qquad a, b, c, d \in \mathbb{C} \quad og \quad ad - bc \neq 0,$$

kalles en LFT (Linear Fractional Transformation). Den **modulære gruppa** består av alle LFT'er som har $a, b, c, d \in \mathbb{Z}$ og $ad-bc = 1$. Lar vi $f_1(z) = \frac{a_1z+b_1}{c_1z+d_1}$ og $f_2(z) = \frac{a_2z+b_2}{c_2z+d_2}$ så får vi ved en utregning at

$$\begin{aligned} f_1 \circ f_2(z) &= \frac{a_1\left(\frac{a_2z+b_2}{c_2z+d_2}\right)+b_1}{c_1\left(\frac{a_2z+b_2}{c_2z+d_2}\right)+d_1} = \frac{a_1\left(a_2z+b_2\right)+b_1(c_2z+d_2)}{c_1\left(a_2z+b_2\right)-d_1(c_2z+d_2)} \\ &= \frac{(a_1a_2+b_1c_2)z+(a_1b_2+b_1d_2)}{(c_1a_2+d_1c_2)z+(c_1b_2+d_1d_2)}. \end{aligned}$$

Tar vi de to matrisene $\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ og $\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$ og multipliserer de så ser vi at

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2+b_1c_2 & a_1b_2+b_1d_2 \\ c_1a_2+d_1c_2 & c_1b_2+d_1d_2 \end{pmatrix}.$$

Nå er $\frac{-az-b}{-cz-d} = \frac{az+b}{cz+d}$ så vi ser at den modulære gruppa er isomorf med $PSL_2(\mathbb{Z})$=$SL_2(\mathbb{Z})/\{I, -I\}$, den projektive spesielle lineære gruppa, som består av 2×2-matriser med determinant lik 1 og hvor matriseparene A og $-A$ identifiseres.

Proposisjon 1. *$SL_2(\mathbb{Z})$ er generert av de to matrisene*

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad og \qquad B = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$$

Bevis. Anta at vi har en 2×2-matrise $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. Vi har $C = AB^5 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $MA = \begin{pmatrix} -b & a \\ -d & c \end{pmatrix}$ og $MC^n = \begin{pmatrix} a & na+b \\ c & nc+d \end{pmatrix}$. Første del av beviset går ut på å multiplisere M med A og C til vi får en matrise på formen $\begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}$.

Hvis $|d| = |c|$ så er $MC^nA = \begin{pmatrix} -na-b & a \\ 0 & c \end{pmatrix}$ for en $n \in \{-1, 1\}$.

Hvis $|d| < |c|$ sett $(s_{ij}) = S_1 = MA$ og hvis $|d| > |c|$ sett $(s_{ij}) = S_1 = M$. Man velger deretter en n_1 slik at $|n_1 s_{21}^1 + s_{22}^1| < |s_{21}^1|$ og setter $S_2 = S_1 C^{n_1} A$. Nå er $|s_{21}^2| < |s_{22}^2|$ og $|s_{21}^2| < |s_{21}^1|$. Så lenge $s_{21}^{p-1} \neq 0$ velger vi en passende n_{p-1} og setter $S_p = S_{p-1} C^{n_{p-1}} A$. Da får vi at $|s_{21}^p| < |s_{21}^{p-1}|$. $\{|s_{22}^n|\}$ er en avtagende følge med 0 som nedre skranke. Det følger at det ekisterer en p slik at $s_{21}^{p+1} = 0$ og $s_{21}^t \neq 0$ for $t < p+1$.

Vi kan altså skrive $MA^{q_1}C^{n_1}AC^{n_2}A...C^{n_p}A = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = R$ for $q_1 \in \{0, 1\}$. R har determinant lik 1 og det følger derfor at $a' = d' = \pm 1$. $A^2 = -I$ så $RA^{q_2}C^n = I$ for en $q_2 \in \{0, 2\}$ og $n(q_2) \in \{b', -b'\}$. Det følger at
$M = C^{n(q_2)} A^{-q_2} A^3 C^{-n_p} ... A^3 C^{-n_2} A^3 C^{-n_1} A^{-q_1}$. □

I $PSL_2(\mathbb{Z})$ er $A^2 = B^3 = I$ så $\langle A \rangle \sim \mathbb{Z}_2$ og $\langle B \rangle \sim \mathbb{Z}_3$. La $PSL_2(\mathbb{Z})$ virke på $\mathbb{R}^2$ og sett $X_1 = 0 \times \mathbb{R}$ og $X_2 = \mathbb{R} \times 0$. Da er $\langle A \rangle X_2 \subseteq X_1$ og $\langle B \rangle X_1 \subseteq X_2$. Ved ping-pong-lemmaet er da $PSL_2(\mathbb{Z})$ isomorf med det frie produktet $\mathbb{Z}_2 * \mathbb{Z}_3$.

3 Representasjoner

La V være et vektorrom over $\mathbb{C}$ og la $GL(V)$ være gruppa av isomorfier fra V på seg selv. Hvis V har en endelig basis (e_i) av n elementer så er hver avbildning $A : V \longrightarrow V$ definert ved en $n \times n$-matrise (a_{ij}). For hvert element i basisen er $A(e_j) = \sum_i a_{ij} e_i$. Gruppa $GL(V)$ kan derfor identifiseres med gruppa av **invertible matriser av orden n**. En **lineær representasjon** av G i V er en homomorfi ρ fra gruppa G inn i gruppa $GL(V)$. For hvert element i $s \in G$ har vi et element $\rho(s) \in GL(V)$, eller ρ_s, slik at

$$\rho(s_1 s_2) = \rho(s_1)\rho(s_2) \ \forall \ s_1, s_2 \in G.$$

Det følger da umiddelbart at

$$\rho(1) = I_n \text{ og } \rho(s^{-1}) = \rho(s)^{-1}.$$

Når ρ er gitt kaller vi V et **representasjonsrom**, eller bare en **representasjon**, av G. Anta nå at V har endelig dimensjon n. Da sier vi at graden til den lineære representasjonen fra G inn i $GL(V)$ er n.

La ρ og ρ' være to representasjoner av samme gruppe G inn i $GL(V)$ og $GL(V')$. Vi sier at disse representasjonene er **isomorfe** hvis det eksisterer en lineær isomorfi $\tau : V \longrightarrow V'$ slik at

$$\tau \circ \rho(s) = \rho'(s) \circ \tau \iff \tau \circ \rho(s) \circ \tau^{-1} = \rho'(s) \qquad \forall\, s \in G.$$

Eksempler:

- En representasjon av grad 1 av en gruppe G er en homomorfi $\rho : G \longrightarrow \mathbb{C}^*$. Hvis gruppa er endelig har ethvert element i $s \in G$ endelig orden og ettersom $s^m = 1$ for en $m \in \mathbb{N}$ så er $\rho_s^m = 1$ og ρ_s er en enhetsrot for alle $s \in G$.

- Hvis vi setter $\rho(s) = 1$ for alle $s \in G$ så får vi en representasjon kalt den trivielle representasjonen.

- La G være endelig av orden g, V være et vektorrom av dimensjon g med en basis $(e_s)_{s \in G}$ indeksert over elementene i G. For $s \in G$ la ρ_s være den lineære avbildningen fra V inn i V som sender e_t på e_{st}. Dette definerer en lineær representasjon kalt den regulære representasjonen av G.

La $\rho : G \longrightarrow GL(V)$ være en representasjon og W være et underrom av V. Vi sier at W er **stabilt**, eller **invariant**, under G hvis $\rho_s x \in W$ for alle $x \in W$ og $s \in G$. Restriksjonen ρ_s^W av ρ_s til W er da en isomorfi av W på seg selv og vi har $\rho_{st}^W = \rho_s^W \rho_t^W$. Derfor er $\rho^W : G \longrightarrow GL(W)$ en lineær representasjon og W kalles en **underrepresentasjon** av V.

Teorem 1. *La $|G| < \infty$ og $\rho : G \longrightarrow GL(V)$ være en representasjon og W være et stabilt underrom av V under G. Da eksisterer et komplement W^c til W i V som er stabilt under G.*

Bevis. Se [1] □

En representasjon V kalles **irredusibel**, eller **simpel**, hvis V ikke har noe invariant, propert underrom under virkning av G. Ved å bruke teorem 1 fører dette til følgende teorem:

Teorem 2. *Enhver representasjon er en direkte sum av irredusible representasjoner.*

Bevis. La V være en lineær representasjon av G. Teoremet bevises ved induksjon på $\dim V$. Teoremet er opplagt for $\dim V = 0$ (0 er den direkte summen av den tomme familien av irredusible representasjoner). Anta derfor at $\dim V \geq 1$. Det er ingenting å bevise hvis V er irredusibelt. Vi antar derfor at V er redusibelt og har et invariant propert underrom W. Ved teorem 1 kan V skrives som en direkte sum av $W \bigoplus W^c$ hvor $\dim W < \dim V$ og $\dim W^c < \dim V$. Ved induksjonshypotesen er W og W^c en direkte sum av irredusible representasjoner og det følger at V også er det. □

La $A = (a_{ij})$ være en $n \times n$-matrise. Trasen til A, t_A, er summen av egenverdiene til A, talt med multiplisiteter, eller ekvivalent $t_A = \sum_{i=1}^{n} a_{ii}$.

La $\rho : G \longrightarrow GL(V)$ være en representasjon av en endelig gruppe i V og sett

$$\chi_\rho(s) = t_{\rho_s}.$$

Den komplekse funksjonen χ_ρ kalles **karakteren** til ρ.

Proposisjon 2. *For karakteren χ til en representasjon ρ av grad n gjelder følgende:*

(i) $\chi(1) = n$

(ii) $\chi(s^{-1}) = \overline{\chi(s)}$

(iii) $\chi(tst^{-1}) = \chi(s)$.

Bevis. Se [1] □

En svært viktig grunn til innføringen av karakteren er at karakteren kan brukes til å skille klasser av representasjoner fra hverandre. Dette kommer til å bli brukt senere i oppgava.

Proposisjon 3. *To representasjoner med samme karakter er isomorfe.*

Bevis. Se [1] □

4 Traseringen

Det **karakteristiske polynomet** til en $n \times n$-matrise A er
$f(\lambda) = Det(A - \lambda I_n) = d_{A-\lambda I_n}$. Egenverdiene til A er løsningene på den **karakteristiske likningen** $f(\lambda) = 0$. Ser vi på tilfellet $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ får vi at

$$\begin{aligned} Det\left(\begin{bmatrix} a-\lambda & b \\ c & d-\lambda \end{bmatrix}\right) &= ad - a\lambda - \lambda d + \lambda^2 - bc \\ &= \lambda^2 - (a+d)\lambda + (ad - bc) = \lambda^2 - t_A\lambda + d_A. \end{aligned}$$

For en 3×3-matrise A kan man regne ut på akkurat samme måte at

$$d_{A-\lambda I} = \lambda^3 - t_A\lambda^2 + \frac{1}{2}(t_A^2 - t_{A^2})\lambda - d_A.$$

Neste teorem skal vi bruke til å vise at enhver potens av en $n \times n$-matrise A kan skrives som en lineær kombinasjon av $A^{n-1}, A^{n-2}, \ldots, I$ med koeffesienter generert av determinanten og trasen.

Teorem 3 (Cayley-Hamilton). *La A være en lineær operator på et endeligdimensjonalt vektorrom V, og la $f(\lambda)$ være det karakteristiske polynomet til A. Da er $f(A) = 0$.*

Bevis. Se [3] □

Ved å bruke Cayley-Hamiltons teorem har vi at $A^2 = t_A \cdot A - d_A \cdot I_2$ for en 2×2-matrise A. For enhver $n > 2$ er $A^n = A^{n-2} \cdot A^2 = A^{n-2} \cdot (t_A \cdot A - d_A) = t_A \cdot A^{n-1} - d_A \cdot A^{n-2}$. Det betyr at etter et endelig antall iterasjoner kan man skrive A^n som en lineær kombinasjon av A og I_2.

Definér binomialkoeffesienten $\binom{n}{i} = 0$ for $i < 0$ og $\sum_i$ til kun å summere over heltall. Da har vi følgende proposisjon.

Proposisjon 4. *La A være en 2×2-matrise. Da har vi at*

$$A^n = \sum_{i=1}^{\frac{n}{2}+1} t_A^{n+1-2i}(-d_A)^{i-1} \binom{n-i}{n+1-2i} \cdot A + \sum_{i=1}^{\frac{n}{2}} t_A^{n-2i}(-d_A)^i \binom{n-1-i}{n-2i} \cdot I_2$$

Bevis. Proposisjonen skal bevises ved induksjon og vi må håndtere de to tilfellene hvor n er odde og n er par separat. Vi regner først ut for $n = 3$ for å se om det stemmer i dette tilfellet.

$$A^3 = t_A \cdot A^2 - d_A \cdot A = t_A \cdot (t_A \cdot A - d_A \cdot I_2) - d_A \cdot A = (t_A^2 - d_A) \cdot A - t_A d_A \cdot I_2$$

Ved å sette $n = 3$ i formelen ovenfor får vi

$$\begin{aligned} A^3 &= \sum_{i=1}^{\frac{3}{2}+1} t_A^{3+1-2i}(-d_A)^{i-1} \binom{3-i}{3+1-2i} \cdot A + \sum_{i=1}^{\frac{3}{2}} t_A^{3-2i}(-d_A)^i \binom{3-1-i}{3-2i} \cdot I_2 \\ &= \sum_{i=1}^{2} t_A^{2(2-i)}(-d_A)^{i-1} \binom{3-i}{2(2-i)} \cdot A + \sum_{i=1}^{1} t_A^{3-2i}(-d_A)^i \binom{2-i}{3-2i} \cdot I_2 \\ &= t_A^2 \cdot A + (-d_A) \cdot A + t_A d_A I_2 = (t_A^2 - d_A) \cdot A - t_A d_A \cdot I_2 \end{aligned}$$

og det er riktig for $n = 3$. Antar vi nå at det stemmer for en vilkårlig $n \geq 3$ så vil vi, med litt regning, finne ut at det også stemmer for $n + 1$. $\square$

4.1 Traser til grupper på to generatorer

La $A = \mathbb{C}[x_1, ..., x_m]$ og $A' = \mathbb{C}[x_{ij}^k]$, $1 \leq i, j \leq n$, $1 \leq k \leq m$ være polynomringer i henholdsvis m og mn^2 variable. Vi kan lage en avbildning $\phi : A \longrightarrow M_n(A')$ ved

$$\phi(x_k) = \begin{pmatrix} x_{11}^k & x_{12}^k & \cdots & x_{1n}^k \\ x_{21}^k & x_{22}^k & \cdots & x_{2n}^k \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1}^k & x_{n2}^k & \cdots & x_{nn}^k \end{pmatrix}.$$

Sett $S = \mathbf{Im}\ \phi$, ringen generert av matrisene $\begin{pmatrix} x_{11}^k & x_{12}^k & \cdots & x_{1n}^k \\ x_{21}^k & x_{22}^k & \cdots & x_{2n}^k \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1}^k & x_{n2}^k & \cdots & x_{nn}^k \end{pmatrix}$ for alle k.

S kalles ringen av m generiske $n \times n$-matriser. La $C_n^m \subseteq A'$ være ringen generert av alle t_s hvor $s \in S$. C_n^m kalles **traseringen** av grad n til m generiske matriser.

Gruppa $GL_n(V)$ virker på S ved $g * s = gsg^{-1}$ for $g \in G$, $s \in S$. Vi vet at $d_{AB} = d_A d_B$ og $t_{ABC} = t_{CAB}$. Det følger da at $d_{BAB^{-1}} = d_A$ og $t_{BAB^{-1}} = t_A$. Det vil si at både trasen og determinanten er invariant under virkning av $GL_n(V)$. Trasene til to isomorfe representasjoner er derfor like. Det samme gjelder for determinantene til to isomorfe representasjoner. La I_n^m være ringen generert av bildet til funksjoner $f : S \longrightarrow A'$ som er invariante under virkning av $GL_n(V)$.

Teorem 4. *Invariantringen I_m^n er lik traseringen C_m^n.*

Bevis. Vi vet at $C_m^n \subseteq I_m^n$. Det motsatte ble antatt av Artin [6] og bevist av Procesi [7]. □

La a og b være generatorene til en gruppe G, $\rho : G \longrightarrow M_n(\mathbb{C})$ og bruk notasjonen $t_a = t_{\rho(a)}$ osv. Nå er $t_{ABC} = t_{CBA}$ så for å finne et generelt uttrykk for t_w for et ord w i G så holder det å se på ordene som er syklisk uavhengige. Ordene i G er på formen $a^{q_0}b^{q_1}a^{q_2}b^{q_3}...a^{q_n-1}b^{q_n}$ hvor $q_i \in \mathbb{Z}$ for $1 \leq i \leq n$.

Nå lar vi $n = 2$ og ser på de 2-dimensjonale representasjonene. Ved Cayley-Hamilton vet vi at $A^2 = t_A \cdot A - d_A \cdot I_2$. Det følger at

$$t_{A^2} = Tr(t_A \cdot A - d_A \cdot I_2) = t_A^2 - 2d_A \Longrightarrow d_A = \frac{t_A^2 - t_{A^2}}{2}.$$

Det vil si at determinanten selv er en trase. Anta nå at vi har et ord $a^{q_0}b^{q_1}a^{q_2}b^{q_3}...a^{q_n-1}b^{q_n}$ som ovenfor. Ved å bruke Cayley-Hamilton kan vi erstatte a^2 (henholdsvis b^2) med $t_a a - d_a I$ (henholdsvis $t_b b - d_b I$). Det følger at ordet kan brytes ned på formen $\sum_{i=1}^{n} k_i a_i bab...ab_i$ hvor $a_i \in \{1, a\}$, $b_i \in \{1, b\}$ og $k_i \in \mathbb{C}[t_a, d_a, t_b, d_b]$. Det vil derfor holde å se på monomene på formen $a_i bab...ab_i$. Ser vi nå på $t_{a_i bab...ab_i} = t_{bab...ab_i a_i} = t_{b_i a_i bab...a}$ ser vi at hvis $b_i = 1 \neq a_i$ eller $b_i \neq 1 = a_i$ så vil trasen til $a_i bab...ab_i$ være lik trasen til $bab..aba^2$ eller $b^2ab..a$ som igjen kan brytes ned. Det vil si at trasen til ethvert ord kan skrives som en linær kombinasjon av trasene til monomer av formen $(ab)^q$, a og b med koeffesienter $k \in \mathbb{C}[t_a, d_a, t_b, d_b]$.

Proposisjon 5. *Traseringen $C_2^2 = \mathbb{C}[t_a, t_{a^2}, t_b, t_{b^2}, t_{ab}]$.*

Bevis. Ved proposisjon 4 har vi et uttrykk for $(ab)^q$ ved hjelp av t_{ab} og d_{ab}. Det følger at $\mathbb{C}[t_a, d_a, t_b, d_b, t_{ab}] = \mathbb{C}[t_a, t_{a^2}, t_b, t_{b^2}, t_{ab}] = C_2^2$. □

Korollar 1. *Traseringen C_2^2 til den modulære gruppa er lik $\mathbb{C}[t_{ab}]$*

Bevis. I tilfellet hvor $a^2 = b^3 = 1$ er de fire andre trasene allerede bestemt. For eksempel er $t_{a^2} = t_1 = 2$ og $t_a = 0$ ved Cayley Hamiltons teorem. Tilsvarende gjør man for t_b og t_{b^2}. □

5 Irredusible representasjoner av den modulære gruppa og undergrupper

La G være en gruppe generert av a og b, og $\rho : G \longrightarrow GL(V) \backsimeq M_n(\mathbb{C})$ være en representasjon av grad n.

Proposisjon 6. *ρ er irredusibel hvis og bare hvis* $\dim \mathbf{Im}\ \rho = n^2$.

Bevis. Sett $P = \mathbf{Im}\ \rho$.

"$\Rightarrow$": $Pv = V\ \forall\ 0 \neq v \in V$ ettersom Pv er et underrom. Altså er ρ surjektiv og $\dim \mathbf{Im}\ \rho = n^2$.

"$\Leftarrow$": La $0 \neq u \in U$, hvor U er et underrom av V. Da har vi at $V = Pu \subseteq U$ og ρ er irredusibel. $\square$

For $n = 1$ er dette trivielt. For $n = 2$ så må $\dim \mathbf{Im}\ \rho = 4$. Regningen fra avsnitt 4.1 viser at den 2-dimensjonale representasjonen av et ord i G vil være en lineær kombinasjon av 1, a, b og ab med koeffesienter $k \in \mathbb{C}[t_a, d_a, t_b, d_b]$. Det betyr at $\{\rho_1, \rho_a, \rho_b, \rho_{ab}\}$ må utspenne $M_2(\mathbb{C})$. Bruker vi notasjonen fra tidligere vil dette være ekvivalent med at vektorene $\{\begin{bmatrix}1\\0\\0\\1\end{bmatrix}, \begin{bmatrix}a_{11}\\a_{12}\\a_{21}\\a_{22}\end{bmatrix}, \begin{bmatrix}b_{11}\\b_{11}\\b_{11}\\b_{11}\end{bmatrix}, \begin{bmatrix}a_{11}b_{11}+a_{12}b_{21}\\a_{11}b_{12}+a_{12}b_{22}\\a_{21}b_{11}+a_{22}b_{21}\\a_{21}b_{12}+a_{22}b_{22}\end{bmatrix}\}$ er lineært uavhengige. Det er tilfellet når

$$Det\left(\begin{pmatrix}1 & a_{11} & b_{11} & a_{11}b_{11}+a_{12}b_{21}\\ 0 & a_{12} & b_{12} & a_{11}b_{12}+a_{12}b_{22}\\ 0 & a_{21} & b_{21} & a_{21}b_{11}+a_{22}b_{21}\\ 1 & a_{22} & b_{22} & a_{21}b_{12}+a_{22}b_{22}\end{pmatrix}\right) = Det\,(A.B - B.A) \neq 0,$$

hvor den første likheten bare er utregning. Dette beviser følgende resultat:

Proposisjon 7. 2×2*-matrisene I,A,B og AB utspenner* $M_2(\mathbb{C})$ *hvis og bare hvis* $Det\,(A.B - B.A) \neq 0$

5.1 1-dimensjonale irredusible representasjoner

La oss først se på de 1-dimensjonale representasjonene av den modulære gruppa. Generatorene a og b oppfyller $a^2 = b^3 = 1$ så $\rho_a^2 = \rho_b^3 = 1$ for enhver 1-dimensjonal representasjon $\rho : G \longrightarrow \mathbb{C}^*$. Ettersom multiplikasjon er kommutativt i $\mathbb{C}$ så vil isomorfe representasjoner være identisk like. Vi ser at $\rho(a) = \pm 1$ og $\rho(b) = \sqrt[3]{1}$ og vi har da i alt seks unike 1-dimensjonale representasjoner. Tabellen under viser de seks representasjonene.

	$\rho(b) = 1$	$\rho(b) = \omega$	$\rho(b) = \omega^2$
$\rho(a) = 1$	ρ_1	ρ_2	ρ_3
$\rho(a) = -1$	ρ_4	ρ_5	ρ_6

5.2 2-dimensjonale irredusible representasjoner

Når vi kommer til det 2-dimensjonale tilfellet blir det straks vanskeligere. Ved å se på utledningen ovenfor har vi at $a^2 = b^3 = 1$ krever $t_a = 0$, $d_a = -1$,

$t_b^2 - d_b = 0$ og $t_b d_b = -1$. Noe som gir $t_b = \sqrt[3]{-1}$ og $d_b = t_b^2$. Det vil si trasen til a^p og b^q er gitt for alle p, q.

Lar vi $\rho_a = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ og løser likningene $t_a = 0$ og $d_a = -1$ får vi løsningene

$$A_1 = \begin{pmatrix} a_{1,11} & \frac{1-a_{1,11}^2}{a_{1,21}} \\ a_{1,21} & -a_{1,11} \end{pmatrix}, \qquad A_2 = \begin{pmatrix} 1 & a_{2,12} \\ 0 & -1 \end{pmatrix} \qquad og \qquad A_3 \begin{pmatrix} -1 & a_{3,12} \\ 0 & 1 \end{pmatrix}.$$

Lar vi på samme måte $\rho_b = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$ og løser likningene $t_b = \sqrt[3]{-1}$ og $d_b = t_b^2$ får vi

$$B_1 = \begin{pmatrix} b_{1,11} & -\frac{b_{1,11}^2+b_{1,11}+1}{b_{1,21}} \\ b_{1,21} & -b_{1,11} - 1 \end{pmatrix} \qquad og \qquad B_2 = \begin{pmatrix} \omega & b_{2,12} \\ 0 & \omega^2 \end{pmatrix},$$

når $t_b = -1$ og $d_b = 1$. For $t_b = \nu$ og $d_b = \nu^2 = \omega$ har vi

$$B_3 = \begin{pmatrix} b_{3,11} & \frac{-b_{3,11}^2+\nu b_{3,11}+\nu^{-1}}{b_{3,21}} \\ b_{3,21} & -b_{3,11} + \nu \end{pmatrix}, \qquad B_4 = \begin{pmatrix} 1 & b_{4,12} \\ 0 & \omega \end{pmatrix} \qquad og \qquad B_5 \begin{pmatrix} \omega & b_{5,12} \\ 0 & 1 \end{pmatrix}.$$

Hvis ρ_a og ρ_b er øvre-triangulære så vil representasjonen opplagt ikke være irredusibel. Vi har derfor 9 kombinasjoner som er mulige kandidater.

$\rho_a^1 = A_1$	$\rho_b^1 = B_1$
$\rho_a^2 = A_1$	$\rho_b^2 = B_2$
$\rho_a^3 = A_1$	$\rho_b^3 = B_3$
$\rho_a^4 = A_1$	$\rho_b^4 = B_4$
$\rho_a^5 = A_1$	$\rho_b^5 = B_5$
$\rho_a^6 = A_2$	$\rho_b^6 = B_1$
$\rho_a^7 = A_2$	$\rho_b^7 = B_3$
$\rho_a^8 = A_3$	$\rho_b^8 = B_1$
$\rho_a^9 = A_3$	$\rho_b^9 = B_3$

Ved uttregningen ovenfor har vi at trasen til ethvert ord er entydig bestemt av de fem trasene $\{t_a, t_{a^2}, t_b, t_{b^2}, t_{ab}\}$. Ved korollar 3 ser vi da at to representasjoner er like dersom de fem tilhørende trasene er like. Det holder derfor å se på karakteren til de fem ordene a, a^2, b, b^2 og ab. Vi vet at $t_a = 0$ og $t_{a^2} = 2$ for alle representasjonene. Vi bruker notasjonen $\chi_s^i = Tr(\rho^i(s))$ og får tabellen

	b	b^2	ab
χ^1	-1	-1	$\frac{2a_{11}b_{11}a_{21}b_{21}-b_{21}^2a_{11}^2+b_{21}^2-a_{21}^2b_{11}^2-a_{21}^2b_{11}-a_{21}^2+a_{11}a_{21}b_{21}}{a_{21}b_{21}}$
χ^2	-1	-1	$a_{11}\omega + a_{21}b_{12} - a_{11}\omega^2$
χ^3	ν	ν^{-1}	$\frac{2a_{11}b_{11}a_{21}b_{21}-b_{21}^2a_{11}^2+b_{21}^2-a_{21}2b_{11}^2+a_{21}^2b_{11}\nu^+a_{21}^2\nu^{-1}-a_{11}a_{21}b_{21}\nu}{a_{21}b_{21}}$
χ^4	ν	ν^{-1}	$a_{11} + a_{21}b_{12} - a_{11}\omega$
χ^5	ν	ν^{-1}	$a_{11}\omega + a_{21}b_{12} - a_{11}$
χ^6	-1	-1	$2b_{11} + a_{12}b_{21} + 1$
χ^7	ν	ν^{-1}	$2b_{11} + a_{12}b_{21} - \nu$
χ^8	-1	-1	$-2b_{11} + a_{12}b_{21} - 1$
χ^9	ν	ν^{-1}	$-2b_{11} + a_{12}b_{21} + \nu$

I tabellen ovenfor ser vi at χ^i_{ab} har mange frie parametere for alle i. Det betyr at vi kan fastsette alle parameterne utenom én og fortsatt kunne generere alle representasjonene. Det er derfor tre klasser av irredusible representasjoner som aldri er isomorfe:

$$\rho_a^1 = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \qquad \rho_b^1 = \begin{pmatrix} \omega & s \\ 0 & \omega^2 \end{pmatrix}$$
$$\rho_a^2 = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \qquad \rho_b^2 = \begin{pmatrix} 1 & t \\ 0 & \omega \end{pmatrix}$$
$$\rho_a^3 = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \qquad \rho_b^3 = \begin{pmatrix} 1 & u \\ 0 & \omega^2 \end{pmatrix}.$$

Representasjonen er irredusibel hvis $Det(AB - BA) \neq 0$. Det vil si så lenge $s \notin \{0, -2(2\omega + 1)\}$, $t \notin \{0, 2(\omega - 1)\}$ og $u \notin \{0, 2(\omega^2 - 1)\}$. Karaktertabellen til de tre representasjonene ser slik ut:

	1	a	b	b^2	ab
χ^1	2	0	-1	-1	$s + 2\omega + 1$
χ^2	2	0	$1 + \omega$	$1 + \omega^2$	$t + 1 - \omega$
χ^3	2	0	$1 + \omega^2$	$1 + \omega$	$u + 1 - \omega^2$

5.3 3-dimensjonale irredusible representasjoner

For $n = 3$ er bildet av $\{1, a, b, b^2, ab, ba, b^2a, bab, b^2ab\}$ en lineær basis for for $M_3(\mathbb{C})$[5]. Det betyr at representasjonen til et hvert ord kan skrives som en lineær kombinasjon av representasjonene til basisen. Karakteren til en representasjon er da kun avhengig av karakteren til disse 9 monomene. Ved å løse likningene gitt ved $\rho_a^2 = 1$, $\rho_b^3 = 1$ og Cayley-Hamilton får vi

$$a^3 = t_a a^2 - \frac{1}{2}(t_a^2 - t_{a^2})a + d_a = a \quad \Longrightarrow \quad t_a = \pm 1$$
$$b^3 = t_b b^2 - \frac{1}{2}(t_b^2 - t_{b^2})b + d_b = 1 \quad \Longrightarrow \quad t_b = t_{b^2} = 0.$$

Akkurat som i tilfellet med $n = 2$ er nå karakteren til representasjonen til noen av ordene bestemt. Ved å se på de 9 monomene som utgjør basisen for $M_3(\mathbb{C})$ så har vi at $t_{ab} = t_{ba}$, $t_{b^2a} = t_{bab}$ og $t_{b^2ab} = t_a$. Det betyr at karakteren til en representasjon er éntydig bestemt av trasen til $\{1, a, b, b^2, ab, b^2a\}$ hvorav trasen til de fire første er bestemt. Ved regning, ved hjelp av f. eks Maple, ser man at matriser som oppfyller Cayley-Hamilton-kravene for a og b har henholdsvis minst 2 og 3 parametere. Trasen til ab og b^2a inneholder minst 2 av disse for alle tilfellene. Man kan på samme måte som med $n = 2$ redusere representasjonene ned til to klasser ved passende konjugasjon og valg av parametre. De to klassene av representasjonene er

$$\rho_a^1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \qquad \rho_b^1 = \begin{pmatrix} s & 1+s-s^2+2t & s+t+st \\ 1 & 1-s & 1+t \\ 0 & -2 & -1 \end{pmatrix}$$
$$\rho_a^2 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \rho_b^2 = \begin{pmatrix} u & 1+u-u^2+2r & u+r+ur \\ 1 & 1-u & 1+r \\ 0 & -2 & -1 \end{pmatrix}.$$

Ved å bruke Shemesh's teorem kan vi finne ut når representasjonene ikke er irredusible.

Teorem 5 (Shemesh's teorem). *[4] De to 3×3-matrisene A og B genererer $M_3(\mathbb{C})$ hvis og bare hvis*

$$\sum_{i,j=1}^{2} [A^i, B^j]^*[A^i, B^j] \qquad \textit{og} \qquad \sum_{i,j=1}^{2} [A^i, B^j][A^i, B^j]^*$$

er invertible.

Her er $[A, B] = AB - BA$ og A^* er den hermittiske transponeringa til A. I tilfellet vårt er $A^2 = 1$, derfor blir likningene redusert til $[A, B]^*[A, B] + [A, B^2]^*[A, B^2]$ og $[A, B][A, B]^* + [A, B^2][A, B^2]^*$. Ved å ta determinanten til disse matrisene og sette den lik 0 finner vi ut at ρ_1 og ρ_2 er redusible for linjene

$$s_1(t) = -1 - t, \qquad s_2(t) = 1 + \omega + 2\omega t \qquad \textit{og} \qquad s_3(t) = 1 + \omega^2 + 2\omega^2 t$$

og

$$u_1(r) = -1 - r, \qquad u_2(r) = 1 + \omega + 2\omega r \qquad \textit{og} \qquad u_3(r) = 1 + \omega^2 + 2\omega^2 r.$$

De 3 linjene krysser hverandre i $(-\frac{1}{2}, 1)$, (ω, ω^2) og (ω^2, ω). Karaktertabellen til de to representasjonene ser slik ut:

	1	a	b	b^2	ab	b^2a
χ^1	3	-1	0	0	$2s$	$2+4t+2s$
χ^2	3	1	0	0	$-2u$	$-2-4r-2u$

5.4 Irredusible representasjoner av gruppa (2,3,p)

La oss ta for oss de tre klassene med 2-dimensjonale representasjoner vi har ovenfor. Ved å løse $(ab)^p = 1$ for forskjellige verdier av p kan vi finne 2-dimensjonale representasjoner av gruppene $(2,3,p)$. Noen tilfeldige eksempler er

$$
\begin{aligned}
p = 2, \qquad & \rho_a = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \qquad \rho_b = \begin{pmatrix} \omega & -2\omega - 1 \\ 0 & \omega^2 \end{pmatrix} \\
p = 6, \qquad & \rho_a = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \qquad \rho_b = \begin{pmatrix} 1 & \omega - 1 \\ 0 & \omega \end{pmatrix} \\
p = 12, \qquad & \rho_a = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \qquad \rho_b = \begin{pmatrix} 1 & \omega - 1 - i\omega^2 \\ 0 & \omega \end{pmatrix}.
\end{aligned}
$$

Så fort $(ab)^p = 1$ er bestemt for en p så er også karakteren til ab bestemt. Det følger derfor fra proposisjon 4 at vi har et endelig antall 2-dimensjonale representasjoner av gruppa $(2,3,p)$.

Ved å bruke de to klassene av representasjoner av dimensjon 3 kan man på samme måte finne representasjoner for forskjellige verdier av p. Noen tilfeldige eksempler på 3-dimensjonale representasjoner er

$$
\begin{aligned}
p = 3, \qquad & \rho_a = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \qquad \rho_b = \begin{pmatrix} 0 & 0 & \frac{-1}{2} \\ 1 & 1 & \frac{1}{2} \\ 0 & -2 & -1 \end{pmatrix} \\
p = 4, \qquad & \rho_a = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \rho_b = \begin{pmatrix} \frac{1}{2} & \frac{1}{4} & \frac{-1}{4} \\ 1 & \frac{1}{2} & \frac{1}{2} \\ 0 & -2 & -1 \end{pmatrix} \\
p = 5, \qquad & \rho_a = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \rho_b = \begin{pmatrix} \nu + 2 & -\nu^2 - 3\nu - 2 & \frac{\nu+1}{2} \\ 1 & -\nu - 1 & \frac{1}{2} \\ 0 & -2 & -1 \end{pmatrix}.
\end{aligned}
$$

6 Ekstensjoner

La G være en gruppe og $\rho : G \longrightarrow GL(V)$ være en representasjon. Vi kan lage en ringhomomorfi $\overline{\rho} : R \longrightarrow End_{\mathbb{C}}(V)$, hvor $R = \mathbb{C}G$, ved $\overline{\rho}(\sum_g a_g g) = \sum_g a_g \rho(g)$, $a_g \in \mathbb{C}, g \in G$. Ved valg av en basis for V vil $End_{\mathbb{C}}(V) \simeq M_n(\mathbb{C})$.

La V og W være to $\mathbb{C}$-vektorrom av dimensjon n og m, og $\rho_1 : G \longrightarrow GL(V)$ og $\rho_2 : G \longrightarrow GL(W)$. Vi kan se på V og W som R-moduler ved å definere $rv = \overline{\rho_1}(r)v$ og $rw = \overline{\rho_2}(r)w$ for $r \in R$ og $v \in V, w \in W$.

En **ekstensjon** av en modul V med en modul W er en korteksakt sekvens av moduler

$$0 \longrightarrow W \longrightarrow E \longrightarrow V \longrightarrow 0.$$

En ekstensjon E er **ekvivalent** med E' dersom det er likheter for W og V og en isomorfi Γ mellom E og E'.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & W & \longrightarrow & E & \longrightarrow & V & \longrightarrow & 0 \\ & & \Big\downarrow{\scriptstyle id} & & \Big\downarrow{\scriptstyle \Gamma} & & \Big\downarrow{\scriptstyle id} & & \\ 0 & \longrightarrow & W & \longrightarrow & E' & \longrightarrow & V & \longrightarrow & 0 \end{array}$$

Den enkleste ekstensjonen er den direkte summen $E = W \bigoplus V$ med inklusjon og projeksjon:

$$0 \longrightarrow W \xrightarrow{\iota} W \bigoplus V \xrightarrow{\pi} V \longrightarrow 0.$$

Ved å bruke representasjonene ρ_1 og ρ_2 til V og W kan man lage en representasjon ρ til $W \bigoplus V$ som er en utvidelse av de to. Det betyr at som R-modul må $(\rho_2(r)w, 0) = \iota(\rho_2(r)w) = \rho(r)\iota(w) = \rho(r)(w,0)$ og $\pi(\rho(r)(0,v)) = \rho_1(r)\pi(0,v) = \rho_1(r)\pi(\beta(r,v),v) = \rho_1(r)v$ for en funksjon $\beta : R \times V \longrightarrow W$.

La $r, s \in R$ og $v \in V$. β må være linær i begge variable og vi har at

$$\begin{aligned} &(\beta(rs,v), rsv) = rs(0,v) = r(\beta(s,v), sv) \\ &= r(\beta(s,v),0) + r(0,sv) = (r\beta(s,v) + \beta(r,sv), rsv). \end{aligned}$$

Definér $\beta_r : V \longrightarrow W$ ved $\beta_r(v) = \beta(r,v)$ og $\varphi : R \longrightarrow Hom_{\mathbb{C}}(V,W)$ ved at $\varphi(r) = \beta_r$ og $(\varphi(r)s)(v) = \beta_r(sv)$. Da ser vi at φ er en derivasjon, $\varphi \in Der_{\mathbb{C}}(R, Hom_{\mathbb{C}}(V,W))$.

Hvis vi har en en ekvivalent ekstensjon så finnes det en isomorfi Γ slik at

$$\begin{array}{ccccccccc} 0 & \longrightarrow & W & \xrightarrow{\iota} & W \bigoplus V & \xrightarrow{\pi} & V & \longrightarrow & 0 \\ & & \Big\downarrow{\scriptstyle id} & & \Big\downarrow{\scriptstyle \Gamma} & & \Big\downarrow{\scriptstyle id} & & \\ 0 & \longrightarrow & W & \xrightarrow{\iota} & W \bigoplus V & \xrightarrow{\pi} & V & \longrightarrow & 0 \end{array}$$

er et kommutativt diagram. Det betyr at $\Gamma \circ \iota(w) = \iota \circ id(w) = (w,0)$, $\pi \circ \Gamma(0,v) = id \circ \pi(0,v) = v$ og $\Gamma(w,v) = (w + \psi(v), v) = \begin{pmatrix} 1 & \psi \\ 0 & 1 \end{pmatrix}$ hvor $\psi \in Hom_{\mathbb{C}}(V,W)$ ved samme utregning som ovenfor. Γ må også ha en R-modul struktur slik at $\Gamma(r(w,v)) = r\Gamma(w,v)$ for alle $r \in R$. Det følger at $r\psi - \psi r = 0$.

Den enkleste utvidete representasjonen er $\rho = \rho_2 \bigoplus \rho_1 = \begin{pmatrix} \rho_2 & 0 \\ 0 & \rho_1 \end{pmatrix}$. En isomorf representasjon vil da være på formen $\Gamma\rho\Gamma^{-1} = \begin{pmatrix} \rho_2 & \psi\rho_1 - \rho_2\psi \\ 0 & \rho_1 \end{pmatrix}$.

De indre derivasjonene, $Inder_{\mathbb{C}}(R, Hom_{\mathbb{C}}(V,W))$, er definért ved

$$D \in Inder_{\mathbb{C}}(R, Hom_{\mathbb{C}}(V,W)) \Longleftrightarrow \exists \quad \psi \in Hom_{\mathbb{C}}(V,W); \quad D(r) = \psi r - r\psi \quad \forall \quad r \in R.$$

De indre derivasjonene tilsvarer basisskifter og

$$Ext^1_R(V,W) := Der_{\mathbb{C}}(R, Hom_{\mathbb{C}}(V,W))/Inder_{\mathbb{C}}(R, Hom_{\mathbb{C}}(V,W)).$$

Representasjoner vi er interessert i vil derfor se ut som $\begin{pmatrix} \rho_2 & \overline{\varphi} \\ 0 & \rho_1 \end{pmatrix}$, hvor $\overline{\varphi} \in Ext^1_R(V,W)$.

6.1 Ekstensjoner av 1-dimensjonale representasjoner

La G være den modulære gruppa. Grupperingen $\mathbb{C}G$ er isomorf med ringen $R = \mathbb{C}[a,b]/(a^2-1, b^3-1)$ så vi kan betrakte R som grupperingen vår. Vi betrakter de to 1-dimensjonale $\mathbb{C}$-vektorrommene V og W som R-moduler ved bruk av to av de 1-dimensjonale representasjonene av den modulære gruppa. Vi lager en ekstensjon av V med W:

$$0 \longrightarrow W \longrightarrow W \bigoplus V \longrightarrow V \longrightarrow 0$$

og vil finne representasjoner $\rho : G \longrightarrow GL(W \bigoplus V)$ hvor $GL(W \bigoplus V) \simeq M_2(\mathbb{C})$ ved valg av basis. En representasjon vil da se ut som $\begin{pmatrix} \rho_2 & \overline{\varphi} \\ 0 & \rho_1 \end{pmatrix}$ hvor $\overline{\varphi} \simeq t \in \mathbb{C}$ ettersom en $Hom_{\mathbb{C}}(V,W) \simeq \mathbb{C}$.

Vi kan se på de seks 1-dimensjonale representasjonene som punkter, hvor vi assosierer ρ_2 med $(1,\omega)$ osv.

$$\begin{array}{ccc} \bullet(1,1) & \bullet(1,\omega) & \bullet(1,\omega^2) \\ \\ \bullet(-1,1) & \bullet(-1,\omega) & \bullet(-1,\omega^2) \end{array}$$

Når vi skal utvide to av de 1-dimensjonale representasjonene kan vi velge to punkter ut av de seks. Det er 15 måter å parre disse på, men det er kun 6 som gir en representasjon som ikke nødvendigvis er en direkte sum.

Proposisjon 8. $Ext^1_R(V,W) = 0$ *hvis og bare hvis punktene har ulik 1. og 2. koordinat.*

Bevis. Vi tar for oss de tre tilfellene hvor punktene har lik 1. koordinat, har lik 2. koordinat og har helt forskjellige koordinater. Uansett hvilke representanter vi velger, vil utregning og resultat bli likt. Vi ser derfor på tre muligheter.

Utvider vi ρ_4 med ρ_5, begge med lik 1. koordinat, får vi

$$\begin{aligned} 0 &= \varphi(0) = \varphi(a^2-1) = a\varphi(a) + \varphi(a)a \\ &= \rho_5(a)\varphi(a) + \varphi(a)\rho_4(a) = -2\varphi(a) \\ &\Longrightarrow \varphi(a) = 0 \\ 0 &= \varphi(0) = \varphi(b^3-1) = b^2\varphi(b) + b\varphi(b)b + \varphi(b)b^2 \\ &= \rho_5(b)^2\varphi(b) + \rho_5(b)\varphi(b)\rho_4(b) + \varphi(b)\rho_4(b)^2 = (1+\omega+\omega^2)\varphi(b) = 0 \\ &\Longrightarrow \varphi(b) \text{ kan velges fritt.} \end{aligned}$$

De indre derivasjonene gir oss

$$\begin{aligned}[a,\psi] &= a\psi - \psi a = 0\\ [b,\psi] &= b\psi - \psi b = (\omega - 1)\psi.\end{aligned}$$

Det betyr at $(0,\varphi(b))/(0,(\omega-1)\psi) \simeq 0$, $\overline{\varphi} = 0$ og representasjonen er på formen $\begin{pmatrix}\rho_5 & 0\\ 0 & \rho_4\end{pmatrix}$, en triviell ekstensjon.

Prøver vi å utvide to som har lik 2. koordinat, for eksempel ρ_1 med ρ_4, så får vi

$$\begin{aligned}0 &= \rho_4(a)\varphi(a) + \varphi(a)\rho_1(a) = 0 \quad \Longrightarrow \varphi(a) \text{ kan velges fritt}\\ 0 &= \rho_4(b)^2\varphi(b) + \rho_4(b)\varphi(b)\rho_1(b) + \varphi(b)\rho_1(b)^2 = 3\varphi(b) \quad \Longrightarrow \varphi(b) = 0\end{aligned}$$

De indre derivasjonene gir oss

$$\begin{aligned}[a,\psi] &= a\psi - \psi a = -2\psi\\ [b,\psi] &= b\psi - \psi b = 0.\end{aligned}$$

Det gir nå at $(\varphi(a),0)/(-2\psi,0) \simeq 0$, $\overline{\varphi} = 0$ og representasjonen er på formen $\begin{pmatrix}\rho_5 & 0\\ 0 & \rho_4\end{pmatrix}$.

Velger vi derimot to representasjoner som har ulike representasjoner for både a og b blir det annerledes. Tar vi ρ_2 med ρ_6:

$$\begin{aligned}0 &= \rho_6(a)\varphi(a) + \varphi(a)\rho_2(a) = 0 \quad \Longrightarrow \varphi(a) \text{ kan velges fritt}\\ 0 &= \rho_6(b)^2\varphi(b) + \rho_6(b)\varphi(b)\rho_2(b) + \varphi(b)\rho_2(b)^2 = (1+\omega+\omega^2)\varphi(b) = 0 \Longrightarrow \varphi(b) \text{ kan velges fritt.}\end{aligned}$$

De indre derivasjonene gir oss

$$\begin{aligned}[a,\psi] &= a\psi - \psi a = -2\psi\\ [b,\psi] &= b\psi - \psi b = (\omega^2 - \omega)\psi.\end{aligned}$$

Dette gir $(\varphi(a),\varphi(b))/(-2\psi,(\omega^2-\omega)\psi) \simeq \mathbb{C}$ og representasjonen er på formen $\begin{pmatrix}\rho_5 & \varphi\\ 0 & \rho_4\end{pmatrix}$, hvor $\varphi(a)$ og $\varphi(b)$ er lineært avhengig og minst én er ulik 0. □

Alle representasjonene vil ha lik karakter for a, mens karakteren for b vil være $1+\omega$, $1+\omega^2$ og -1. Dette er de samme karakterene som for de 2-dimensjonale irredusible representasjonene vi har funnet tidligere. De utvidete representasjonene er indekomposable, men ikke irredusible. De er øvre triangulære for både a og b.

Referanser

[1] Serre, J.-P.: *Linear Representations of Finite Groups* Springer-Verlag New York, 1977

[2] Friedberg, A. H., Insel A. J., Spence, L. E.: *Linear Algebra* Illinois State University side 317

[3] Artin, M.: *On Azumaya Algebras and Finite Dimensional Representations of Rings. Journal of Algebra 11 side 532-563* 1969

[4] Procesi, C.: *The invariant theory of* $n \times n$ *matrices. Adv. in math. 19 side 306-381* 1976

[5] Sletsjøe, A. B.: *Finite dimensional representations of the projective modular group* math.AG/0610587

[6] Aslaksen, H., Sletsjøe, A. B.: *Generators of matrix algebras in dimension 2 and 3* Linear Algebra and its Applications 430 2009